Discrete Mathematics 67 (1987) 101–105
North-Holland

NOTE

CONGRUENCES IN Z^n, FINITE ABELIAN GROUPS AND THE CHINESE REMAINDER THEOREM

M.A. FIOL

Department of Mathematics, E.T.S.I. Telecommunication, Polytechnic University of Catalonia, Spain

Received 9 February 1984
Revised 30 October 1986

A natural generalization to Z^n of the concept of congruence leads to the consideration of finite Abelian groups whose structure is obtained from the Smith normal form theorem for integral matrices. Moreover, the characterization of the group generators allows us to prove simply a result which turns out to be a generalization of the Chinese remainder theorem.

1. Introduction

Let $\mathbf{Z}$ and $\mathbf{Z}^{n\times n}$ be the rings of integers and $n \times n$ matrices over $\mathbf{Z}$ respectively. Let $\mathbf{Z}^n$ denote the additive group of column n-vectors with integral coordinates. Its elements will also be referred as points.

Let $M = (m_{ij})$ be a matrix of $\mathbf{Z}^{n\times n}$ with linearly independent columns $\boldsymbol{m}^j = (m_{1j}, m_{2j}, \ldots, m_{nj})^{\mathrm{T}}$, $j = 1, 2, \ldots, n$, that is $m = \det M \neq 0$. The set $M\mathbf{Z}^n$, whose elements are a linear combination (with integral coefficients) of the vectors $\boldsymbol{m}^j$, is said to be the *lattice* generated by M. Clearly, $M\mathbf{Z}^n$ with the usual vector addition is a normal subgroup of $\mathbf{Z}^n$.

Let $k \in \mathbf{Z}$, $1 \leqslant k \leqslant n$. The kth *determinantal divisor* of M, denoted by $d_k(M) = d_k$, is defined as the greatest common divisor of all the $\binom{n}{k}^2$ $k \times k$ determinantal minors of M. Since M is nonsingular, not all of them are zero. Note that $d_k \mid d_{k+1}$ for all k and $d_n = |m|$. For convenience, put $d_0 = 1$. The *invariant factors* of M are the quantities

$$s_k(M) = s_k = \frac{d_k}{d_{k-1}}, \quad k = 1, 2, \ldots, n.$$

It can be shown that $s_i \mid s_{i+1}$, $i = 1, 2, \ldots, n-1$, see [3].

By the Smith normal form theorem, M is equivalent to the diagonal matrix $S(M) = S = \mathrm{diag}(s_1, s_2, \ldots, s_n)$, that is there exist two unimodular (with determinant ± 1) integral matrices, U and V, such that $S = UMV$. For more details, see [3].

As usual, $(a_1, a_2, \ldots, a_n)$ denotes the g.c.d. of the integers $a_1, a_2, \ldots, a_n$. When we consider them as the coordinates of a vector $\boldsymbol{a}$, we will write $(\boldsymbol{a})$.

2. Congruences in $\boldsymbol{Z}^n$

Let $\alpha, \beta, m \in \boldsymbol{Z}$, $m \neq 0$. Using the standard notation, $\alpha \equiv \beta \pmod{m}$ means that

$$\alpha - \beta \in m\boldsymbol{Z}, \tag{1}$$

where $m\boldsymbol{Z}$ denotes the ideal of $\boldsymbol{Z}$ formed by the multiples of m. This suggests the following natural generalization to $\boldsymbol{Z}^n$ of the concept of congruence (for some properties related to this concept, see [2]).

Let $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{Z}^n$. Let $M \in \boldsymbol{Z}^{n \times n}$ be a nonsingular matrix with $m = \det M$. We say that $\boldsymbol{a}$ is congruent with $\boldsymbol{b}$ modulo M, and write $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{M}$ if

$$\boldsymbol{a} - \boldsymbol{b} \in M\boldsymbol{Z}^n, \tag{2}$$

that is, the point $\boldsymbol{a} - \boldsymbol{b}$ belongs to the lattice generated by M.

Some straightforward consequences of this definition follow in the next proposition. Throughout, $\boldsymbol{0}$ represents the zero vector.

Proposition 1. *Let $\alpha, \beta \in \boldsymbol{Z}$ and $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \boldsymbol{Z}^n$. Then,*

(a) $\alpha \equiv \beta \pmod{m} \Rightarrow \alpha\boldsymbol{a} \equiv \beta\boldsymbol{a} \pmod{M}$,

(b) $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{M}$, $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{M} \Rightarrow \alpha\boldsymbol{a} + \beta\boldsymbol{c} \equiv \alpha\boldsymbol{b} + \beta\boldsymbol{d} \pmod{M}$.

Note that, by (2) and (1), whenever $M = \operatorname{diag}(m_1, m_2, \ldots, m_n)$ the vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^{\mathrm{T}}$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)^{\mathrm{T}}$ are congruent modulo M iff the system of congruences (in $\boldsymbol{Z}$)

$$a_i \equiv b_i \pmod{m_i}, \quad i = 1, 2, \ldots, n, \tag{3}$$

holds.

3. The group $\boldsymbol{Z}^n/M\boldsymbol{Z}^n$

Since $M\boldsymbol{Z}^n \lhd \boldsymbol{Z}^n$, we can consider the quotient group $\boldsymbol{Z}^n/M\boldsymbol{Z}^n$. It can intuitively be called the *group of integral vectors modulo M*. Henceforth, we follow the usual convention of identifying each equivalence class by any of its representatives.

To find the structure of $\boldsymbol{Z}^n/M\boldsymbol{Z}^n$, note firstly that, if $M = \operatorname{diag}(m_1, m_2, \ldots, m_n)$, this group is the direct product of the cyclic groups $\boldsymbol{Z}/m_i\boldsymbol{Z}$, $i = 1, 2, \ldots, n$.

Let us now consider the Smith normal form of M, $S = \operatorname{diag}(s_1, s_2, \ldots, s_n) = UMV$. Then, replacing M by $U^{-1}SV^{-1}$ in (2), and recalling that U, V (and hence

U^{-1}, V^{-1}) are unimodular, we conclude after some simple manipulations that $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{M}$ iff

$$\boldsymbol{u}_i\boldsymbol{a} \equiv \boldsymbol{u}_i\boldsymbol{b} \pmod{s_i}, \quad i = 1, 2, \ldots, n, \tag{4}$$

where $\boldsymbol{u}_i$, $i = 1, 2, \ldots, n$, stands for the ith row of U.

Assume now that p is the smallest integer such that $s_{n-p} = 1$ ($\Rightarrow s_1 = s_2 = \cdots = s_{n-p-1} = 1$). Then, the first $n-p$ equations in (4) are irrelevant, and we only need to consider the others, that is

$$U'\boldsymbol{a} \equiv U'\boldsymbol{b} \pmod{S'}, \tag{5}$$

where U' is the $p \times n$ matrix obtained from U by leaving out the first $n-p$ rows, and $S' = \operatorname{diag}(s_{n-p+1}, s_{n-p+2}, \ldots, s_n)$.

So, the (linear) mapping ϕ between the vectors modulo M and the vectors modulo S' given by $\phi(\boldsymbol{a}) = U'\boldsymbol{a}$ is well-defined, preserves addition, and is a bijection. Therefore ϕ is a group isomorphism, and we can write

$$\boldsymbol{Z}^n/M\boldsymbol{Z}^n \cong \bigtimes_{i=n-p+1}^{n} \boldsymbol{Z}/s_i\boldsymbol{Z}. \tag{6}$$

As, for any finite Abelian group G, it is trivial to find a matrix $M \in \boldsymbol{Z}^{n\times n}$ such that $G \cong \boldsymbol{Z}^n/M\boldsymbol{Z}^n$, (6) is nothing more than the decomposition theorem for finite Abelian groups, where the s_i represent the invariant factors of G.

The next proposition contains two easy consequences of the above.

Proposition 2. (a) *The number of equivalence classes modulo M is*

$$\mathrm{o}(\boldsymbol{Z}^n/M\boldsymbol{Z}^n) = |\det M|.$$

(b) *The group $\boldsymbol{Z}^n/M\boldsymbol{Z}^n$ is cyclic iff $d_{n-1} = 1$.*

Given an element $\boldsymbol{a}$ of $\boldsymbol{Z}^n/M\boldsymbol{Z}^n$, we are interested in finding its order, $\mathrm{o}(\boldsymbol{a}) = \mathrm{o}(\langle \boldsymbol{a} \rangle)$, that is, the smallest positive integer γ such that $\gamma\boldsymbol{a} \equiv \boldsymbol{0} \pmod{M}$ or, equivalently,

$$\gamma M^{-1}\boldsymbol{a} = \frac{|m|\, M^{-1}\boldsymbol{a}}{|m|/\gamma} \in \boldsymbol{Z}^n$$

where $m = \det M$. Since γ is minimum, $|m|/\gamma$ (index of $\langle \boldsymbol{a} \rangle$) is the maximum positive integer that divides m and also all the numbers $\boldsymbol{m}_i\boldsymbol{a}$, $i = 1, 2, \ldots, n$ ($\boldsymbol{m}_i$ denotes the ith row of $mM^{-1} = M^{adj}$). With our notation, $|m|/\gamma = (m, (mM^{-1}\boldsymbol{a}))$. Thus,

$$\mathrm{o}(\boldsymbol{a}) = \frac{|m|}{(m, (mM^{-1}\boldsymbol{a}))}. \tag{7}$$

Note that, if $n = 1$, M and $\boldsymbol{a}$ are integers, say m and α respectively. Then $M^{-1} = m^{-1}$, and (7) particularizes to $\mathrm{o}(\boldsymbol{a}) = |m|/(m, \alpha)$.

Let us now see a generalization of Proposition 1(a) in which the order of an element plays a significant role. Let $\alpha, \beta \in \mathbf{Z}$, $\boldsymbol{a} \in \mathbf{Z}^n$ and $M \in \mathbf{Z}^{n\times n}$ (M nonsingular). Then $(\alpha-\beta)\boldsymbol{a} \equiv \mathbf{0} \pmod{M}$ holds iff $o(\boldsymbol{a})$ divides $\alpha-\beta$. So, we have

Proposition 3. $\alpha\boldsymbol{a} \equiv \beta\boldsymbol{a} \pmod{M} \Leftrightarrow \alpha \equiv \beta \pmod{o(\boldsymbol{a})}$.

4. The Chinese remainder theorem

A slightly generalized version of the Chinese remainder theorem is the following (see, for instance, [1]):

Let $b_1, b_2, \ldots, b_n$ be arbitrary integers. Let $m_1, m_2, \ldots, m_n$ and $a_1, a_2, \ldots, a_n$ be integers such that

$$(m_i, m_j) = 1, \quad i \neq j, \tag{8a}$$

$$(a_i, m_i) = 1, \quad i = 1, 2, \ldots, n. \tag{8b}$$

Then, the system of congruences

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, 2, \ldots, n, \tag{9}$$

has exactly one solution modulo $m = m_1 m_2 \cdots m_n$.

According to the last remark in Section 2, the system (9) is equivalent to the congruence in $\mathbf{Z}^n$

$$x\boldsymbol{a} \equiv \boldsymbol{b} \pmod{M}, \tag{10}$$

where $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^{\mathrm{T}}$, $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)^{\mathrm{T}}$ and $M = \mathrm{diag}(m_1, m_2, \ldots, m_n)$.

Stated in this form, it is apparent that (13) has always (for any $\boldsymbol{b}$) a solution iff the group $\mathbf{Z}^n/M\mathbf{Z}^n$ is cyclic and the vector $\boldsymbol{a}$ generates it, that is $o(\boldsymbol{a}) = |m|$ or, from (9),

$$(m, (mM^{-1}\boldsymbol{a})) = 1. \tag{11}$$

Moreover, if this condition holds, Proposition 3 implies that any two solutions are congruent modulo m.

The above argument holds true independently of whether or not M is diagonal. Therefore, we can state the following generalization of the Chinese remainder theorem:

Theorem (Chinese remainder theorem). *Given a matrix $M \in \mathbf{Z}^{n\times n}$ with $m = \det M \neq 0$, if $(m, (mM^{-1}\boldsymbol{a})) = 1$, then the congruence $x\boldsymbol{a} = \boldsymbol{b} \pmod{M}$ has exactly one solution modulo m.*

When M is the aforementioned diagonal matrix, $m = m_1 m_2 \cdots m_n$ and (11) results into

$$\left(m, \frac{a_1 m}{m_1}, \ldots, \frac{a_n m}{m_n}\right) = 1, \tag{12}$$

a condition that can be easily proved equivalent to (8a) and (8b).

On the other hand, if $\boldsymbol{Z}^n/M\boldsymbol{Z}^n$ is cyclic, $s_n = |m|$ (Proposition 2(b)) and $S = \text{diag}(1, 1, \ldots, 1, |m|) = UMV$ for some unimodular matrices $U, V \in \boldsymbol{Z}^{n\times n}$. So, the group isomorphism discussed in Section 3 is

$$\phi : \boldsymbol{Z}^n/M\boldsymbol{Z}^n \to \boldsymbol{Z}/m\boldsymbol{Z}, \qquad \boldsymbol{a} \to \phi(\boldsymbol{a}) = \boldsymbol{u}_n \boldsymbol{a},$$

where $\boldsymbol{u}_n$ denotes the nth row of U, and (10) is equivalent (has the same solutions) to

$$x\boldsymbol{u}_n \boldsymbol{a} \equiv \boldsymbol{u}_n \boldsymbol{b} \pmod{m}.$$

This congruence has exactly one solution modulo m if

$$(\boldsymbol{u}_n \boldsymbol{a}, m) = 1, \tag{13}$$

that, together with $s_n = |m|$ (or $d_{n-1} = 1$), is clearly equivalent to (11). Moreover, this solution is given by

$$x = (\boldsymbol{u}_n \boldsymbol{b})(\boldsymbol{u}_n \boldsymbol{a})^{-1}. \tag{14}$$

Conclusions

In the same way as the quotient structures induced by congruence in $\boldsymbol{Z}$ are the cyclic groups, the finite Abelian groups appear when we deal with the generalization of that concept in $\boldsymbol{Z}^n$. In this context, the theory of integral matrices proves to be very useful in deriving the properties related with such concepts.

Although in this paper we have restricted ourselves to the ring of integers, no essential modification is required to extend all the results to the case of any *principal ideal ring* (that is, any commutative ring with no zero divisors such that every ideal is principal).

References

[1] T.M. Apostol, Introduction to Analytic Number Theory (Springer, New York, 1976).

[2] M.A. Fiol, Applications of graph theory to interconnection networks (in Spanish), Ph. D. Thesis, Polytech. Univ. of Barcelona, Spain (1982).

[3] M. Newman, Integral Matrices, Pure and Appl. Math. Series Vol. 45 (Academic Press, New York, 1972).